

# National Cyber Alert System

[Archive](#)

## Cyber Security Bulletin SB09-187

### Vulnerability Summary for the Week of June 29, 2009

The US-CERT Cyber Security Bulletin provides a summary of new vulnerabilities that have been recorded by the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) in the past week. The NVD is sponsored by the Department of Homeland Security (DHS) National Cyber Security Division (NCSD) / United States Computer Emergency Readiness Team (US-CERT). For modified or updated entries, please visit the [NVD](#), which contains historical vulnerability information.

The vulnerabilities are based on the [CVE](#) vulnerability naming standard and are organized according to severity, determined by the [Common Vulnerability Scoring System](#) (CVSS) standard. The division of high, medium, and low severities correspond to the following scores:

- **High** - Vulnerabilities will be labeled High severity if they have a CVSS base score of 7.0 - 10.0
- **Medium** - Vulnerabilities will be labeled Medium severity if they have a CVSS base score of 4.0 - 6.9
- **Low** - Vulnerabilities will be labeled Low severity if they have a CVSS base score of 0.0 - 3.9

Entries may include additional information provided by organizations and efforts sponsored by US-CERT. This information may include identifying information, values, definitions, and related links. Patch information is provided when available. Please note that some of the information in the bulletins is compiled from external, open source reports and is not a direct result of US-CERT analysis.

High Vulnerabilities					
Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info	
armassa -- ard-9808_software armassa -- ard-9808	The ARD-9808 DVR card security camera allows remote attackers to cause a denial of service via a long URI composed of //.\ (slash slash dot backslash) sequences.	2009-07-02	7.8	<a href="#">CVE-2009-2305</a> MILWoRM	
armassa -- ard-9808_software armassa -- ard-9808	The ARD-9808 DVR card security camera stores sensitive information under the web root with insufficient access control, which allows remote attackers to download a file containing usernames and passwords via a direct request for dvr.ini.	2009-07-02	7.5	<a href="#">CVE-2009-2306</a> MILWoRM	
awesomephp -- mega_file_manager	Directory traversal vulnerability in index.php in Awesome PHP Mega File Manager 1.0 allows remote attackers to include and execute arbitrary local files via a .. (dot dot) in the page parameter. NOTE: in some environments, this can be leveraged for remote file inclusion by using a UNC share pathname or an ftp, ftps, or ssh2.sftp URL.	2009-06-30	7.5	<a href="#">CVE-2009-2263</a> MILWoRM SECUNIA	
biglle -- vote_for_us_extension	SQL injection vulnerability in voteforus.php in the Vote For Us extension 1.0.1 and earlier for PunBB allows remote attackers to execute arbitrary SQL commands via the out parameter.	2009-07-01	7.5	<a href="#">CVE-2009-2276</a> MILWoRM	
bow_dor_klein -- v_blo	SQL injection vulnerability in include/get_read.php in Extensible-BioLawCom CMS (X-BLC) 0.2.0 and	2009-07-	7.5	<a href="#">CVE-2009-2310</a> VIE	

bow_user_kiwiie -- x-dic	earlier allows remote attackers to execute arbitrary SQL commands via the section parameter.	02	7.5	<a href="#">AF</a> <a href="#">BID</a> <a href="#">MILWoRM</a>
codice-cms -- codice_cms	SQL injection vulnerability in index.php in Codice CMS 2 allows remote attackers to execute arbitrary SQL commands via the tag parameter.	2009-07-02	7.5	<a href="#">CVE-2009-2309</a> <a href="#">BID</a> <a href="#">MILWoRM</a>
ez_systems -- ez_publish	The registration view (/user/register) in eZ Publish 3.5.6 and earlier, and possibly other versions before 3.9.5, 3.10.1, and 4.0.1, allows remote attackers to gain privileges as other users via modified ContentObjectAttribute_data_user_login_30, ContentObjectAttribute_data_user_password_30, and other parameters.	2009-07-02	7.5	<a href="#">CVE-2008-6844</a> <a href="#">XF</a> <a href="#">BID</a> <a href="#">OSVDB</a> <a href="#">MILWoRM</a> <a href="#">CONFIRM</a>
giorgio_tani -- peazip	PeaZIP 2.6.1, 2.5.1, and earlier on Windows allows user-assisted remote attackers to execute arbitrary commands via a .zip archive with a .txt file whose name contains   (pipe) characters and a command.	2009-06-30	9.3	<a href="#">CVE-2009-2261</a> <a href="#">MILWoRM</a>
gmitc -- com_dbquery	PHP remote file inclusion vulnerability in the Green Mountain Information Technology and Consulting Database Query (com_dbquery) component 1.4.1.1 and earlier for Joomla! allows remote attackers to execute arbitrary PHP code via a URL in the mosConfig_absolute_path parameter to classes/DBQ/admin/common.class.php.	2009-07-01	7.5	<a href="#">CVE-2008-6841</a> <a href="#">XF</a> <a href="#">BID</a> <a href="#">MILWoRM</a>
hp -- openview_network_node_manager	Stack-based buffer overflow in rping in HP OpenView Network Node Manager (OV NNM) 7.53 on Linux allows remote attackers to execute arbitrary code via unspecified vectors, possibly involving a CGI request to webappmon.exe. NOTE: this may overlap CVE-2009-1420.	2009-07-02	7.5	<a href="#">CVE-2009-2298</a> <a href="#">IDEFENSE</a>
huawei -- d100	The Huawei D100 has (1) a certain default administrator password for the web interface, and does not force a password change; and has (2) a default password of admin for the admin account in the telnet interface; which makes it easier for remote attackers to obtain access.	2009-07-01	10.0	<a href="#">CVE-2009-2271</a> <a href="#">BUGTRAQ</a>
huawei -- d100	The Huawei D100 allows remote attackers to obtain sensitive information via a direct request to (1) lan_status_adv.asp, (2) wlan_basic_cfg.asp, or (3) lancfg.asp in en/, related to use of JavaScript to protect against reading file contents.	2009-07-01	7.8	<a href="#">CVE-2009-2274</a> <a href="#">BUGTRAQ</a>
jinzora -- jinzora	Directory traversal vulnerability in index.php in Jinzora Media Jukebox 2.8 and earlier allows remote attackers to include and execute arbitrary local files via a .. (dot dot) in the name parameter.	2009-07-02	7.5	<a href="#">CVE-2009-2313</a> <a href="#">MILWoRM</a>
joomla -- com_casiino_blackjack joomla -- com_casino_videopoker joomla -- com_casinobase	SQL injection vulnerability in the (1) casinobase (com_casinobase), (2) casino_blackjack (com_casino_blackjack), and (3) casino_videopoker (com_casino_videopoker) components 0.3.1 for Joomla! allows remote attackers to execute arbitrary SQL commands via the Itemid parameter to index.php.	2009-06-27	7.5	<a href="#">CVE-2009-2239</a> <a href="#">XF</a> <a href="#">BID</a> <a href="#">MILWoRM</a>
kim_eckert -- com_bsadv	SQL injection vulnerability in the Boy Scout Advancement (com_bsadv) component 0.3 and earlier for Joomla! allows remote attackers to execute arbitrary SQL commands via the id parameter in a (1)	2009-07-01	7.5	<a href="#">CVE-2009-2290</a> <a href="#">BID</a> <a href="#">BUGTRAQ</a>

	account or (2) event task to index.php.			<a href="#">BUGTRAQ</a>
maxdev -- cwguestbook	SQL injection vulnerability in the CWGuestBook module 2.1 and earlier for MAXdev MDPro (aka MD-Pro) allows remote attackers to execute arbitrary SQL commands via the rid parameter in a viewrecords action to modules.php.	2009-07-02	7.5	<a href="#">CVE-2009-2307</a> <a href="#">XF</a> <a href="#">MILWoRM</a>
motorola -- timbuktu_pro	Stack-based buffer overflow in Motorola Timbuktu Pro 8.6.5 on Windows allows remote attackers to execute arbitrary code by sending a long malformed string over the PlughNTCommand named pipe.	2009-06-26	9.3	<a href="#">CVE-2009-1394</a> <a href="#">BUGTRAQ</a> <a href="#">MISC</a>
myiosoft -- ajaxportal	PHP remote file inclusion vulnerability in install/di.php in AjaxPortal 3.0 allows remote attackers to execute arbitrary PHP code via a URL in the pathtoserverdata parameter. NOTE: the installation instructions specify deleting the install/ folder.	2009-06-30	7.5	<a href="#">CVE-2009-2262</a> <a href="#">BUGTRAQ</a>
nagios -- nagios	statuswml.cgi in Nagios before 3.1.1 allows remote attackers to execute arbitrary commands via shell metacharacters in the (1) ping or (2) Traceroute parameters.	2009-07-01	7.5	<a href="#">CVE-2009-2288</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">SECUNIA</a>
netgear -- dg632	The administrative web interface on the Netgear DG632 with firmware 3.4.0_ap allows remote attackers to cause a denial of service (web outage) via an HTTP POST request to cgi-bin/firmwarecfg.	2009-06-30	7.8	<a href="#">CVE-2009-2256</a> <a href="#">MISC</a> <a href="#">BUGTRAQ</a> <a href="#">BUGTRAQ</a> <a href="#">MILWoRM</a> <a href="#">SECTRACK</a>
netgear -- dg632	The administrative web interface on the Netgear DG632 with firmware 3.4.0_ap allows remote attackers to bypass authentication via a direct request to (1) gateway/commands/saveconfig.html, and (2) stattbl.htm, (3) modemmenu.htm, (4) onload.htm, (5) form.css, (6) utility.js, and possibly (7) indextop.htm in html/.	2009-06-30	7.8	<a href="#">CVE-2009-2257</a> <a href="#">MISC</a> <a href="#">BUGTRAQ</a> <a href="#">MILWoRM</a> <a href="#">SECTRACK</a>
netgear -- dg632 netgear -- dg632_firmware	Directory traversal vulnerability in cgi-bin/webcm in the administrative web interface on the Netgear DG632 with firmware 3.4.0_ap allows remote attackers to list arbitrary directories via a .. (dot dot) in the nextpage parameter.	2009-06-30	7.8	<a href="#">CVE-2009-2258</a> <a href="#">MISC</a> <a href="#">BUGTRAQ</a> <a href="#">MILWORM</a> <a href="#">SECTRACK</a>
phion -- airlock_web_application_firewall	The management interface in the phion airlock Web Application Firewall (WAF) 4.1-10.41 does not properly handle CGI requests that specify large width and height parameters for an image, which allows remote attackers to execute arbitrary commands or cause a denial of service (resource consumption) via a crafted request.	2009-07-02	10.0	<a href="#">CVE-2009-2300</a> <a href="#">MISC</a> <a href="#">BUGTRAQ</a>
phome_empire -- phome_empire_cms	SQL injection vulnerability in Empire CMS 5.1 allows remote attackers to execute arbitrary SQL commands via the bid parameter to the default URI under e/tool/gbook/.	2009-07-01	7.5	<a href="#">CVE-2009-2269</a> <a href="#">BUGTRAQ</a>
punres -- affiliates_mod	Multiple SQL injection vulnerabilities in affiliates.php in the Affiliation (aka Affiliates) module 1.1.0 and earlier for PunBB allow remote attackers to execute	2009-07-02	7.5	<a href="#">CVE-2009-2308</a> <a href="#">XF</a> <a href="#">OSVDB</a> <a href="#">MILWoRM</a>

	arbitrary SQL commands via the (1) in or (2) out parameter.	02		MILWORM SECUNIA MISC MISC
radware -- gateway radware -- appwall	The radware AppWall Web Application Firewall (WAF) 1.0.2.6, with Gateway 4.6.0.2, allows remote attackers to read source code via a direct request to (1) funcs.inc, (2) defines.inc, or (3) msg.inc in Management/.	2009-07-02	7.8	CVE-2009-2301 BUGTRAQ
selbstzweck -- rgallery_plugin	SQL injection vulnerability in the rGallery plugin 1.2.3 for WoltLab Burning Board (WBB3) allows remote attackers to execute arbitrary SQL commands via the userID parameter in the RGalleryUserGallery page to index.php, a different vector than CVE-2008-4627.	2009-07-02	7.5	CVE-2009-2311 XF BID MILWORM
sun -- opensolaris sun -- solaris	The NFSv4 server kernel module in Sun Solaris 10, and OpenSolaris before snv_119, does not properly implement the nfs_portmon setting, which allows remote attackers to access shares, and read, create, and modify arbitrary files, via unspecified vectors.	2009-07-02	10.0	CVE-2009-2296 SUNALERT CONFIRM
sun -- opensolaris sun -- solaris	Unspecified vulnerability in the udp subsystem in the kernel in Sun Solaris 10, and OpenSolaris snv_90 through snv_108, when Solaris Trusted Extensions is enabled, allows remote attackers to cause a denial of service (panic) via unspecified vectors involving the crgetlabel function, related to a "TX panic." NOTE: this issue exists because of a regression in earlier kernel patches.	2009-07-02	7.1	CVE-2009-2297 SUNALERT CONFIRM
tutorial-share -- tutorial_share	Optimum Web Design Tutorial Share 3.5.0 and earlier allows remote attackers to bypass authentication and obtain administrative access by setting the usernamed cookie parameter.	2009-07-01	7.5	CVE-2009-2293 XF BID MILWORM SECUNIA OSVDB
zen-cart -- zen_cart	Zen Cart 1.3.8a, 1.3.8, and earlier does not require administrative authentication for admin/sqlpatch.php, which allows remote attackers to execute arbitrary SQL commands via the query_string parameter in an execute action, in conjunction with a PATH_INFO of password_forgotten.php, related to a "SQL Execution" issue.	2009-06-30	7.5	CVE-2009-2254 XF CONFIRM CONFIRM BID

[Back to top](#)**Medium Vulnerabilities**

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ad2000 -- free-sw_leger	Cross-site scripting (XSS) vulnerability in AD2000 free-sw leger (aka Web Conference Room Free) 1.6.4 and earlier allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	2009-06-27	4.3	CVE-2009-2240 BID CONFIRM SECUNIA JVND JVN
	Cross-site scripting (XSS) vulnerability in Appleple a-News			CVE-2009-2292 XF BID

appleple -- a-news	2.32 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	2009-07-01	4.3	OSVDB CONFIRM SECUNIA JVND JVN
arcadetradescript -- arcade_trade_script	Cross-site scripting (XSS) vulnerability in index.php in Arcade Trade Script 1.0 beta allows remote attackers to inject arbitrary web script or HTML via the q parameter in a gamelist action.	2009-07-01	4.3	CVE-2009-2289 BUGTRAQ MISC SECUNIA
artofdefence -- hyperguard	The Artofdefence Hyperguard Web Application Firewall (WAF) module before 2.5.5-11635, 3.0 before 3.0.3-11636, and 3.1 before 3.1.1-11637, a module for the Apache HTTP Server, allows remote attackers to cause a denial of service (memory consumption) via an HTTP request with a large Content-Length value but no POST data.	2009-07-02	5.0	CVE-2009-2299 BUGTRAQ MISC SECUNIA
avast -- avast_antivirus	Multiple stack-based buffer overflows in avast! Linux Home Edition 1.0.5, 1.0.5-1, and 1.0.8 allow remote attackers to cause a denial of service (application crash) or execute arbitrary code via a malformed (1) ISO or (2) RPM file.	2009-07-02	6.8	CVE-2008-6846 XF
avatic -- aardvark_topsites_php	Cross-site scripting (XSS) vulnerability in index.php in Aardvark Topsites PHP 5.2.0 and earlier allows remote attackers to inject arbitrary web script or HTML via the q parameter in a search action.	2009-07-02	4.3	CVE-2009-2302 XF BID BUGTRAQ MISC
avatic -- aardvark_topsites_php	index.php in Aardvark Topsites PHP 5.2.1 and earlier allows remote attackers to obtain sensitive information via a negative integer value for the start parameter in a search action, which reveals the installation path in an error message.	2009-07-02	5.0	CVE-2009-2303 XF BUGTRAQ MISC
avatic -- aardvark_topsites_php	index.php in Aardvark Topsites PHP 5.2.0 and earlier allows remote attackers to obtain sensitive information via a nonexistent account name in the u parameter in a rate action, which reveals the installation path in an error message.	2009-07-02	5.0	CVE-2009-2304 XF BUGTRAQ MISC
chad_phillips -- logintoboggan	Unspecified vulnerability in LoginToboggan 6.x-1.x before 6.x-1.5, a module for Drupal, when "Allow users to login using their e-mail address" is enabled, allows remote blocked users to bypass intended access restrictions via unspecified vectors.	2009-07-01	6.8	CVE-2009-2291 VUPEN BID CONFIRM CONFIRM
christof_bruyland -- v-webmail	Multiple PHP remote file inclusion vulnerabilities in V-webmail 1.6.4 allow remote attackers to execute arbitrary PHP code via a URL in the (1) CONFIG[pear_dir] parameter to (a) Mail/RFC822.php, (b) Net/Socket.php, (c) XML/Parser.php, (d) XML/Tree.php, (e) Mail/mimeDecode.php, (f) Console/Getopt.php, (g) System.php, (h) Log.php, and (i) File.php in includes/pear/; the CONFIG[pear_dir] parameter to (j) includes/prepend.php, and (k) includes/cachedConfig.php; and the (2) CONFIG[includes] parameter to (l) prepend.php and (m) email.list.search.php in includes/. NOTE: the CONFIG[pear_dir] parameter to includes/mailaccess/pop3.php is already covered by CVE-2006-2666.	2009-07-01	6.8	CVE-2008-6840 XF BID MISC
				CVE-2008-

clamav -- clamav	The unpack feature in ClamAV 0.93.3 and earlier allows remote attackers to cause a denial of service (segmentation fault) via a corrupted LZH file.	2009-07-02	5.0	6845 BID BUGTRAQ MISC OSVDB
cpanel -- cpanel	Directory traversal vulnerability in frontend/x3/stats/lastvisit.html in cPanel allows remote attackers to read arbitrary files via a .. (dot dot) in the domain parameter.	2009-07-01	5.0	CVE-2009-2275 MILWORM
cpanel -- cpanel netenberg -- fantastico_de_luxe	Directory traversal vulnerability in index.php in Fantastico, as used with cPanel 11.x, allows remote attackers to read arbitrary files via a .. (dot dot) in the sup3r parameter.	2009-07-02	5.0	CVE-2008-6843 XF BID BUGTRAQ
dedecms -- dedecms	Unrestricted file upload vulnerability in member/uploads_edit.php in dedecms 5.3 allows remote attackers to execute arbitrary code by uploading a file with a double extension in the filename, then accessing this file via unspecified vectors, as demonstrated by a .jpg.php filename.	2009-07-01	6.8	CVE-2009-2270 BUGTRAQ
freebsd -- freebsd netbsd -- netbsd openbsd -- openbsd	The gdoa (aka new dtoa) implementation in gdoa/misc.c in libc in FreeBSD 6.4 and 7.2, NetBSD 5.0, and OpenBSD 4.5 allows context-dependent attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a large precision value in the format argument to a printf function, related to an "array overrun."	2009-07-01	6.8	CVE-2009-0689 BID CONFIRM SECTRACK CONFIRM
huaweidevice -- d100	The Huawei D100 stores the administrator's account name and password in cleartext in a cookie, which allows context-dependent attackers to obtain sensitive information by (1) reading a cookie file, by (2) sniffing the network for HTTP headers, and possibly by using unspecified other vectors.	2009-07-01	5.0	CVE-2009-2272 BUGTRAQ
huaweidevice -- d100	The default configuration of the Wi-Fi component on the Huawei D100 does not use encryption, which makes it easier for remote attackers to obtain sensitive information by sniffing the network.	2009-07-01	5.0	CVE-2009-2273 BUGTRAQ
james_ashton -- compface	Buffer overflow in compface 1.5.2 and earlier allows user-assisted attackers to cause a denial of service (crash) via a long declaration in a .xbm file.	2009-07-01	4.3	CVE-2009-2286 MLIST MLIST CONFIRM
libtiff -- libtiff	Buffer underflow in the LZWDecodeCompat function in libtiff 3.8.2 allows context-dependent attackers to cause a denial of service (crash) via a crafted TIFF image, a different vulnerability than CVE-2008-2327.	2009-07-01	4.3	CVE-2009-2285 CONFIRM MLIST MLIST MLIST MISC CONFIRM
linux -- kernel	The kvm_arch_vcpu_ioctl_set_sregs function in the KVM in Linux kernel 2.6 before 2.6.30, when running on x86 systems, does not validate the page table root in a KVM_SET_SREGS call, which allows local users to cause a denial of service (crash or hang) via a crafted cr3 value, which triggers a NULL pointer dereference in the gfn_to_rmap function.	2009-07-01	4.9	CVE-2009-2287 MLIST
moefoo smartfilter	SmartFilter Web Gateway Security 4.2.1.00 stores user credentials in cleartext in config.txt and uses insecure	2009-07-01	4.6	CVE-2009-2312 VFE

unace -- smartunzip	permissions for this file, which allows local users to gain privileges.	2009-07-02	4.0	<a href="#">XF SECUNIA FULLDISC</a>
net-snmp -- net-snmp red_hat -- enterprise_linux redhat -- enterprise_linux	agent/snmp_agent.c in snmpd in net-snmp 5.0.9 in Red Hat Enterprise Linux (RHEL) 3 allows remote attackers to cause a denial of service (daemon crash) via a crafted SNMP GETBULK request that triggers a divide-by-zero error. NOTE: this vulnerability exists because of an incorrect fix for CVE-2008-4309.	2009-06-26	5.0	<a href="#">CVE-2009-1887 CONFIRM REDHAT</a>
php-address_book -- php-address_book	Multiple SQL injection vulnerabilities in PHP Address Book 4.0.x allow remote attackers to execute arbitrary SQL commands via (1) the alphabet parameter to index.php or (2) the id parameter to delete.php. NOTE: the view.php and edit.php vectors are already covered by CVE-2008-2565.	2009-06-30	6.8	<a href="#">CVE-2009-2259 BUGTRAQ</a>
php.s3 -- tree_bbs	Cross-site scripting (XSS) vulnerability in Let's PHP! Tree BBS 2004/11/23 and earlier allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	2009-06-26	4.3	<a href="#">CVE-2009-2226 SECUNIA CONFIRM JVNDB JVN</a>
phpmyadmin -- phpmyadmin	Cross-site scripting (XSS) vulnerability in phpMyAdmin before 3.2.0.1 allows remote attackers to inject arbitrary web script or HTML via a crafted SQL bookmark.	2009-07-01	4.3	<a href="#">CVE-2009-2284 CONFIRM</a>
pidgin -- pidgin	The OSCAR protocol implementation in Pidgin before 2.5.8 misinterprets the ICQWebMessage message type as the ICQSMS message type, which allows remote attackers to cause a denial of service (application crash) via a crafted ICQ web message that triggers allocation of a large amount of memory.	2009-07-01	5.0	<a href="#">CVE-2009-1889 MLIST CONFIRM</a>
pluck-cms -- pluck	Directory traversal vulnerability in data/modules/blog/module_pages_site.php in Pluck 4.6.1 allows remote attackers to include and execute arbitrary local files via a .. (dot dot) in the post parameter.	2009-07-02	6.8	<a href="#">CVE-2008-6842 XF BID MILWoRM SECUNIA</a>
preproject -- pre_asp_job_board	Cross-site scripting (XSS) vulnerability in Employee/emp_login.asp in Pre ASP Job Board allows remote attackers to inject arbitrary web script or HTML via the msg parameter.	2009-07-02	4.3	<a href="#">CVE-2008-6847 XF BID MISC</a>
stardict -- stardict	stardict 3.0.1, when Enable Net Dict is configured, sends the contents of the clipboard to a dictionary server, which allows remote attackers to obtain sensitive information by sniffing the network.	2009-06-30	5.0	<a href="#">CVE-2009-2260 BUGTRAQ MISC</a>
sun -- opensolaris sun -- solaris	The Virtual Network Terminal Server daemon (vntsd) for Logical Domains (aka LDoms) in Sun Solaris 10, and OpenSolaris svn_41 through svn_108, on SPARC platforms does not check authorization for guest console access, which allows local control-domain users to gain guest-domain privileges via unknown vectors.	2009-07-01	4.6	<a href="#">CVE-2009-2282 CONFIRM</a>
sun -- java_web_console sun -- solaris	Multiple cross-site scripting (XSS) vulnerabilities in the help.jsp scripts in Sun Java Web Console 3.0.2 through 3.0.5, and Sun Java Web Console in Solaris 10, allow remote attackers to inject arbitrary web script or HTML via unspecified vectors.	2009-07-01	4.3	<a href="#">CVE-2009-2283 SUNALERT CONFIRM</a>
	Zen Cart 1.3.8a, 1.3.8, and earlier does not require administrative authentication for			<a href="#">CVE-2009-</a>

zen-cart -- zen_cart	Administrator authentication for admin/record_company.php, which allows remote attackers to execute arbitrary code by uploading a .php file via the record_company_image parameter in conjunction with a PATH_INFO of password_forgotten.php, then accessing this file via a direct request to the file in images/.	2009-06-30	6.8	2255 XF CONFIRM CONFIRM BID
----------------------	---	------------	-----	---

[Back to top](#)**Low Vulnerabilities**

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
hp -- oncplus	Unspecified vulnerability in NFS / ONCplus on HP HP-UX B.11.31 allows local users to cause a denial of service via unknown attack vectors. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	2009-07-02	2.1	CVE-2009-1421 BID
sun -- java_system_access_manager	Cross-site scripting (XSS) vulnerability in the Cross-Domain Controller (CDC) servlet in Sun Java System Access Manager 6 2005Q1, 7 2005Q4, and 7.1 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	2009-07-01	2.6	CVE-2009-2268 SUNALERT CONFIRM

[Back to top](#)**Last updated July 06, 2009**
 Print This Document